Advantages of embodiments of the present invention include preventing the unauthorized access to secure pages, the stealing of passwords by a third party, the falsification or modification of form data or the replaying of a valid form submission at a later time. Additionally, embodiments of the present invention do not require the licensing of security technology, such as SSL, from a third party vendor, and does not require special support in a user's web browser, such as https. Since authentication packets are transparent to the web server, the present invention can be used to integrate with any third party vendor's security application program interface (API) simply by modifying an applet and the software for an authentication or integration server.

Having thus described at least one illustrative embodiment of the invention, various alterations, modifications and improvements will readily occur to those skilled in the art. Such alterations, modifications and improvements are intended to be within the scope and spirit of the invention. Accordingly, the foregoing description is by way of example only and is not intended as limiting. The invention's limit is defined only in the following claims and the equivalents thereto.

What is claimed is:

1. A method for authenticating a user of a computer, the method comprising:

transmitting a signal having a challenge string and a first encryption key;

receiving a login packet having the challenge string and a password that is encrypted using the first encryption key;

decrypting the password;

receiving information from an authentication provider; and

authenticating the password by using the information received from the authentication provider.

2. The method of claim 1, wherein transmitting a signal having a challenge string comprises transmitting an applet having a sequence number.

3. The method of claim 1, wherein transmitting a signal having a challenge string comprises transmitting an applet having a session identifier.

4. The method of claim 1, wherein receiving a login packet comprises receiving from a computer a login packet having a challenge string, a user name, a password, wherein the challenge string, the user name, and the password are encrypted using the first encryption key.

5. The method of claim 4, wherein receiving a login packet comprises receiving from a computer a login packet having a hash of the session identification, the user name, and the password.

6. A method for authenticating a user of a computer over a computer network, the method comprising:

transmitting to the computer a signal having a unique session identifier and a first encryption key;

receiving from the computer a login packet having the session identification, a user name, a password and a first hash of the session identification, the user name, and the password, wherein the session identification, the user name, and the password are encrypted using the first encryption key;

decrypting the session identification, the user's name, and the password contained in the packet;

receive information from an authentication provider; and

authenticating the user's name and the password by using the information provided by the authentication provider.

7. The method of claim 6, wherein authenticating the user's name and the password by using the information provided by the authentication provider comprises:

receiving from the authentication provider a second encryption key;

encrypting the user name and the password using the second encryption key and transmitting the encrypted user name and password to the authentication provider;

receiving from the authentication provider a second hash of the password and a character string; and

determining from the second hash if the password is correct.

8. The method of claim 6, further comprising:

transmitting to the computer a form and a second unique sequence identification;

receiving, from the computer, response data to the form and a third hash of the second unique sequence identification, the user password, and fields and values entered on the form; and

authenticating the fields and the values entered on the form.

9. The method of claim 6, wherein the authentication provider includes an authentication server.

10. The method of claim 7, wherein the authentication provider includes an authentication server.

11. The method of claim 6, wherein the authentication provider includes a software program in communication with the computer network.

12. The method of claim 6, wherein the authentication provider includes a software program in communication with the computer network.

13. The method of claim 7, wherein the first hash and the second hash both include an MD5 hash.

14. The method of claim 7, further comprising changing the first and the second encryption keys on a predetermined basis.

15. A system for authenticating a user of a computer coupled to a computer network, the system comprising:

a web server coupled to the computer network, wherein the web server is programmed to:

transmit a signal having a challenge string and a first encryption key;

receive a login packet having the challenge string and a password that is encrypted using the first encryption key;

decrypt the password;

receive information from an authentication provider; and

authenticate the password by using the information provided by the authentication provider.

16. The system of claim 15, wherein the signal is an applet and the challenge string includes a sequence number.

17. The system of claim 15, wherein the signal is an applet and the challenge string includes a session identifier.

18. The system of claim 15, wherein the login packet further comprises a user name and the session identification and wherein the user name and the password are encrypted using the first encryption key.

19. The system of claim 18, wherein the login packet further comprises a hash of the session identification, the user name, and the password.

20. A system for authenticating a user of a computer over a computer network coupled to a security server, the system comprising:

a web server coupled to the computer and the computer network, wherein the web server is programmed to:

transmit to the computer a signal having a unique session identification and a first encryption key and;

receive from the computer a login packet having the session identification, a user name, a password and a first hash of the session identification, the user name, and the password, wherein the session identification, the user name, and the password are encrypted using the first encryption key;

decrypt the session identification, the user's name, and the password contained in the packet;

receive information from an authentication provider; and

authenticate the user's name and the password by using the information provided by the authentication provider.

21. The system of claim 20, wherein to authenticate the user's name and the password by using the information provided by the authentication provider, the web server is programmed to:

receive from the authentication provider a second encryption key;

encrypt using the second encryption key and transmit to the authentication provider the user name and the password;

receive from the authentication provider a second hash of the password and a character string; and

determine from the second hash if the password is correct.

22. The system of claim 20, wherein the authentication provider includes an authentication server.

23. The system of claim 20, wherein the authentication provider includes a software program in communication with the computer network.

24. The system of claim 21, wherein the authentication provider includes an authentication server.

25. The system of claim 21, wherein the authentication provider includes a software program in communication with the computer network.

26. The system of claim 20, wherein the web server includes a computer program installed on the computer.

27. The system of claim 21, wherein the first and the second encryption keys are changed on a predetermined basis.

28. An article of manufacture, comprising:

a computer readable medium having computer readable program code for authenticating a user of a client computer over a computer network, the computer readable program code including instructions for:

causing the computer system to transmit a signal having a challenge string and a first encryption key;

causing the computer system to receive a login packet having the challenge string and a password that is encrypted using the first encryption key;

causing the computer system to decrypt the password;

causing the computer system to receive information from an authentication provider; and

causing the computer system to authenticate the password by using the information provided by the authentication provider.

29. The article of manufacture of claim 28, wherein the computer readable program code having instructions for causing the computer system to receive a login packet comprises causing the computer system to receive from a computer a login packet having

a challenge string, a user name, a password, wherein the session identification, the user name, and the password are encrypted using the first encryption key.

30. The method of claim 28, wherein the computer readable program code having instructions for causing the computer system to receive a login packet comprises causing the computer system to receive from a computer a login packet having a hash of the session identification, the user name, and the password.

31. An article of manufacture, comprising:

a computer readable medium having computer readable program code for authenticating a user of a client computer over a computer network, the computer readable program code including instructions for:

causing the computer system to transmit to the client computer a signal having a unique session identification and a first encryption key;

causing the computer system to receive from the client computer a login packet having the session identification, a user name, a password and a first hash of the session identification, the user name, and the password, wherein the session identification, the user name, and the password are encrypted using the first encryption key;

causing the computer system to decrypt the session identification, the user's name, and the password contained in the packet; and

causing the computer system to receive information from an authentication provider; and

causing the computer system to authenticate the user's name and the password by

using the information provided by the authentication provider.

32. The article of manufacture of claim 31, wherein the instructions for causing the computer system to authenticate the user's name and the password by using the information provided by the authentication provider comprises:

causing the computer system to receive from the authentication provider a second encryption key;

causing the computer system to encrypt using the second encryption key and transmit to the authentication provider the user name and the password;

causing the computer system to receive from the authentication provider a second hash of the password and a character string; and

causing the computer system to determine from the character string if the password is correct.

33. The article of manufacture of claim 31, wherein the computer readable program code further comprises instructions for:

causing the computer system to change the first and the second encryption keys on a predetermined basis.

34. The article of manufacture of claim 31, wherein the computer readable program code further comprises instructions for:

causing the computer system to transmit to the client computer a form and a second unique sequence identification;